PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-193569
(43)Date of publication of application : 28.07.1995

(51)Int.Cl. H04L 9/06
H04L 9/14
G06F 13/00
G06F 15/00
H04K 1/00

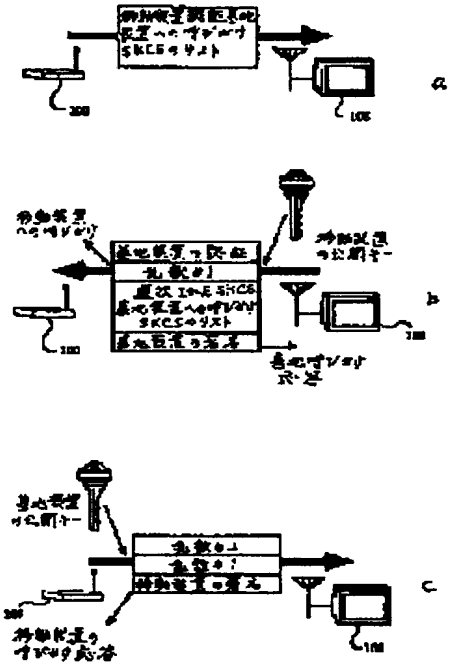
(21)Application number : 06-210786
(22)Date of filing : 12.08.1994

(71)Applicant : SUN MICROSYST INC
(72)Inventor : DIFFIE WHITFIELD
AZIZ ASHAR

(30)Priority
Priority number : 93 147661 Priority date : 02.11.1993 Priority country : US

(54) METHOD FOR KEEPING SAFETY OF COMMUNICATION AND DEVICE FOR SAFELY TRANSFERRING DATA

(57)Abstract:
PURPOSE: To provide the method and device for security communication which are provided with a security radio communication link between a mobile device and a base device.
CONSTITUTION: A mobile device 100 transmits host authentication (Cert Mobile) to a base device 105 together with a call value (CH1) selected at random and a list of supported shared key algorithms (SKCS). The base device 105 discriminates whether the host authentication (Cert Mobile) is valid or not. If it is not valid, the base device 105 rejects the connection attempt. Next, the base device 105 transmits Cert Base, random numbers(RN1) enciphered by a public key of the mobile device 100, and an identifier for selected SKCD to the mobile device 100. The base device 105 preserves random numbers RN1, and the CH1 value and the selected SKCS are added to a message to be transmitted to the base device 105. The mobile device 100 verifies Cert Base, and if this authentication is valid, the mobile device 100 verifies the signature of the message under a public key (Pub Base) of the base device 105.



LEGAL STATUS
[Date of request for examination] 13.08.2001
[Date of sending the examiner's decision of rejection]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平7－193569

(43)公開日　平成７年(1995)７月28日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｌ	9/06				
	9/14				
Ｇ０６Ｆ	13/00	３５１　Ｚ	7368－5B		
	15/00	３３０　Ｂ	7459－5L		
				Ｈ０４Ｌ　9/ 02　Ｚ	

審査請求　未請求　請求項の数４　ＦＤ　（全 16 頁）　最終頁に続く

(21)出願番号　特願平6－210786

(22)出願日　平成６年(1994)８月12日

(31)優先権主張番号　１４７６６１

(32)優先日　1993年11月２日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　591064003
サン・マイクロシステムズ・インコーポレーテッド
ＳＵＮ　ＭＩＣＲＯＳＹＳＴＥＭＳ，ＩＮＣＯＲＰＯＲＡＴＥＤ
アメリカ合衆国　94043　カリフォルニア州・マウンテンビュー・ガルシア　アヴェニュウ・2550

(72)発明者　ホイットフィールド・ディフィー
アメリカ合衆国　94040　カリフォルニア州・マウンテンビュー・ハンス　アヴェニュ・283

(74)代理人　弁理士　山川　政樹

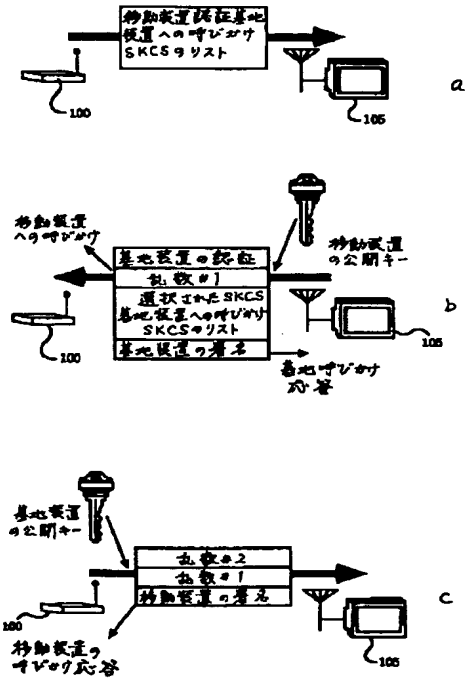
最終頁に続く

(54)【発明の名称】　通信の安全を保つ方法及び安全にデータを転送する装置

(57)【要約】

【目的】　移動装置と基地装置間に機密無線通信リンクを備えた機密保護通信方法及び装置を提供することを目的とする。

【構成】　移動装置１００が、ホスト認証（Ｃｅｒｔ　Ｍｏｂｉｌｅ）をランダムに選択された呼び掛け値（ＣＨ１）及びサポートされた共用キーアルゴリズム（ＳＫＣＳ）のリストと共に基地装置１０５に送信する。基地装置１０５がＣｅｒｔ＿Ｍｏｂｉｌｅが有効か否かを判定する。Ｃｅｒｔ＿Ｍｏｂｉｌｅが有効でないならば、基地装置１０５が接続の試みを拒否する。次に、基地装置１０５がＣｅｒｔ＿Ｂａｓｅ、移動装置１００の公開キーで暗号化された乱数（ＲＮ１）及び選択されたＳＫＣＳための識別子を移動装置１００に送信する。基地装置１０５がＲＮ１を保管し、ＣＨ１値及び選択されたＳＫＣＳを基地装置１０５に送信されたメッセージに付加する。次に、移動装置１００がＣｅｒｔ＿Ｂａｓｅを検証し、認証が有効ならば、移動装置１００がメッセージの署名を基地装置１０５の公開キー（Ｐｕｂ＿Ｂａｓｅ）の下で検証する。



1

【 特許請求の範囲】

【 請求項1 】　第1 のデータ処理装置と第2 のデータ処理装置間で通信の安全を保つ方法において、

（ａ）前記第1 のデータ処理装置は、移動装置の公開キー（Ｐｕｂ＿Ｍｏｂｉｌｅ）、選択された呼び掛け値（ＣＨ1）及びサポートされた共用キーアルゴリズム（ＳＫＣＳ）のリストを含んでいる移動装置の認証（Ｃｅｒｔ＿Ｍｏｂｉｌｅ）を含む第1 のメッセージを第2 のデータ処理装置に送信し、

（ｂ）前記第2 のデータ処理装置は前記第1 のメッセージを受信し、第1 の認証機関（ＣＡ）の第1 の署名を検証し、前記受信されたＣｅｒｔ＿Ｍｏｂｉｌｅを検証し、前記Ｃｅｒｔ＿Ｍｏｂｉｌｅが有効ならば、前記第2 のデータ処理装置は、基地装置の公開キー（Ｐｕｂ＿Ｂａｓｅ）、第2 のディジタル署名、乱数（ＲＮ1）、及び前記サポートされた共用キーアルゴリズムのリストから選択された前記ＳＫＣＳの一つの識別子を含んでいる第2 の基地装置の認証（Ｃｅｒｔ＿Ｂａｓｅ）を含む第2 のメッセージを前記第1 のデータ処理装置に送信し、

（ｃ）前記第1 のデータ処理装置は前記第2 のメッセージを受信し、かつ前記Ｃｅｒｔ＿Ｂａｓｅを検証し、前記Ｃｅｒｔ＿Ｂａｓｅが有効ならば、前記第1 のデータ処理装置は前記Ｐｕｂ＿Ｂａｓｅを使用して前記Ｃｅｒｔ＿Ｂａｓｅの前記第2 のディジタル署名を検証し、前記第2 のディジタル署名が有効ならば、前記第1 のデータ処理装置は前記第1 のデータ処理装置の私用キー（Ｐｒｉｖ＿Ｍｏｂｉｌｅ）を使用してＥ（Ｐｕｂ＿Ｍｏｂｉｌｅ，ＲＮ1）の値を暗号解読することによってＲＮ1 の値を決定し、

（ｄ）前記第1 のデータ処理装置は値ＲＮ2 と値（ＲＮ1 とＲＮ2 とのＥＸ－ＯＲ）を有する第1 のセッションキーとを発生し、前記第1 のデータ処理装置は、前記基地装置の公開キー（Ｐｕｂ＿Ｂａｓｅ）を使用してＲＮ2 の値を暗号化し、前記第1 のデータ処理装置に対応するディジタル署名に加えて前記暗号化されたＲＮ2 及びＥ（Ｐｕｂ＿Ｍｏｂｉｌｅ，ＲＮ1）を含んでいる第3 のメッセージを前記第2 のデータ処理装置に送信し、

（ｅ）前記第2 のデータ処理装置は前記第3 のメッセージを受信し、前記Ｃｅｒｔ＿Ｍｏｂｉｌｅから得られたＰｕｂ＿Ｍｏｂｉｌｅを使用して前記第1 のデータ処理装置の前記ディジタル署名を検証し、前記第1 のデータ処理装置の前記署名が検証されるならば、前記第2 のデータ処理装置は前記第2 のデータ処理装置の私用キー（Ｐｒｉｖ＿Ｂａｓｅ）を使用してＥ（Ｐｕｂ＿Ｂａｓｅ，ＲＮ2）の値を暗号解読し、前記第2 のデータ処理装置は（ＲＮ1 とＲＮ2 とのＥＸ－ＯＲ）の値を有する第1 のセッションキーを使用し、

（ｆ）前記第1 及び第2 のデータ処理装置は前記第1 のセッションキーを使用して暗号解読される暗号化されたデータを使用してデータを転送することを特徴とする通信の安全を保つ方法。

2

【 請求項2 】　複数のＣＡを含み、前記第2 のメッセージが、式{ Ｃｅｒｔ＿Ｐａｔｈ，ＣＲＬのリスト，Ｅ（Ｐｕｂ＿Ｍｏｂｉｌｅ，ＲＮ1），選択されたＳＫＣＳ，Ｓｉｇ（Ｐｒｉｖ＿Ｂａｓｅ，{ Ｅ（Ｐｕｂ＿Ｍｏｂｉｌｅ，ＲＮ1），選択されたＳＫＣＳ，ＣＨ1，ＳＫＣＳのリスト} ）} によって規定され、ＣＲＬは前記ＣＡの各々に対して認証取り消しリストを備えていることを特徴とする請求項1 に記載の通信の安全を保つ方法。

【 請求項3 】　第2 のデータ処理装置と通信する第1 のデータ処理装置を有するネットワークの前記第1 のデータ処理装置と前記第2 のデータ処理装置間で安全にデータを転送する装置において、

移動装置の公開キー（Ｐｕｂ＿Ｍｏｂｉｌｅ）、選択された呼び掛け値（ＣＨ1）及びサポートされた共用キーアルゴリズム（ＳＫＣＳ）のリストを有する移動装置の認証（Ｃｅｒｔ＿Ｍｏｂｉｌｅ）を含む第1 のメッセージを第2 のデータ処理装置に送信するために前記第1 のデータ処理装置に結合された第1 のメッセージ発生・送受信回路と、

前記第1 のメッセージを受信し、前記受信されたＣｅｒｔ＿Ｍｏｂｉｌｅを検証し、前記Ｃｅｒｔ＿Ｍｏｂｉｌｅが有効ならば、基地装置の公開キー（Ｐｕｂ＿Ｂａｓｅ）、第2 のディジタル署名、乱数（ＲＮ1）、及び前記サポートされた共用キーアルゴリズムのリストから選択された前記ＳＫＣＳの一つの識別子を含んでいる基地装置の認証（Ｃｅｒｔ＿Ｂａｓｅ）を含む第2 のメッセージを前記第1 のデータ処理装置に送信する前記第2 のデータ処理装置に結合された第2 のメッセージ発生・送受信回路とを備え、

前記第1 のデータ処理装置は、前記第1 のメッセージ発生及び送受信回路を使用して前記第2 のメッセージを受信し、かつ前記Ｃｅｒｔ＿Ｂａｓｅを検証し、前記Ｃｅｒｔ＿Ｂａｓｅが有効ならば、前記第1 のデータ処理装置は、前記Ｐｕｂ＿Ｂａｓｅを使用して前記メッセージの前記第2 の署名を検証し、前記第2 の署名が有効ならば、前記第1 のデータ処理装置は前記第1 のデータ処理装置の私用キー（Ｐｒｉｖ＿Ｍｏｂｉｌｅ）を使用してＥ（Ｐｕｂ＿Ｍｏｂｉｌｅ，ＲＮ1）の値を暗号解読することによってＲＮ1 の値を決定し、

前記第1 のデータ処理装置は値ＲＮ2 と値（ＲＮ1 とＲＮ2 とのＥＸ－ＯＲ）有する第1 のセッションキーとを発生し、前記第1 のデータ処理装置は、前記基地装置の公開キー（Ｐｕｂ＿Ｂａｓｅ）を使用してＲＮ2 の値を暗号化し、前記第1 のデータ処理装置に対応するディジタル署名に加えて前記暗号化されたＲＮ2 及びＥ（Ｐｕｂ＿Ｍｏｂｉｌｅ，ＲＮ1）を含んでいる第3 のメッセージを前記第2 のデータ処理装置に送信し、

3

前記第2 のデータ処理装置は、前記第2 のメッセージ発生・送受信回路を使用して前前記第3 のメッセージを受信し、前記Ｃｅｒｔ＿Ｍｏｂｉｌｅから得られたＰｕｂ＿Ｍｏｂｉｌｅを使用して前記第1 のデータ処理装置の前記ディジタル署名を検証し、前記第1 のデータ処理装置の前記署名が検証されるならば、前記第2 のデータ処理装置は前記第2 のデータ処理装置の私用キー（Ｐｒｉｖ＿Ｂａｓｅ）を使用してＥ（Ｐｕｂ＿Ｂａｓｅ，ＲＮ２）の値を暗号解読し、前記第2 のデータ処理装置は（ＲＮ1とＲＮ2とのＥＸ－ＯＲ）の値を有する第1 のセッションキーを使用し、

前記第1 及び第2 のデータ処理装置は前記第1 のセッションキーを使用して暗号解読される暗号化されたデータを使用してデータを転送するようにしたことを特徴とする安全にデータを転送する装置。

【請求項4】　複数のＣＡを含み、前記第2 のメッセージは、式{Ｃｅｒｔ＿Ｐａｔｈ，ＣＲＬのリスト，Ｅ（Ｐｕｂ＿Ｍｏｂｉｌｅ，ＲＮ1），選択されたＳＫＣＳ，Ｓｉｇ（Ｐｒｉｖ＿Ｂａｓｅ，{Ｅ（Ｐｕｂ＿Ｍｏｂｉｌｅ，ＲＮ1），選択されたＳＫＣＳ，ＣＨ1，ＳＫＣＳのリスト}）}によって規定され、ＣＲＬは前記ＣＡの各々に対して認証取り消しリストを備えていることを特徴とする請求項3 に記載の安全にデータを転送する装置。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、無線ネットワークにおけるプライバシー及び認証のための方法及び装置に関するものである。特に、本発明は無線移動装置と基地局間の通信のための公開キー及び共用キーの両方の暗号化技術を使用するシステムを提供する。

【０００２】

【従来の技術】ポータブル・パーソナルコンピュータ及びワークステーションの出現は、ネットワークの概念を拡大して移動装置を含ませるようになった。これらの移動装置はグローバルネットワーク間並びにローカルネットワーク内で移動される。例えば、ポータブル・ノートブック計算装置の使用者は、カリフォルニア州パロアルトからタイのバンコックまで物理的に自分のコンピュータを携えることが可能である。そのコンピュータがネットワークに結合される他のコンピュータと対話し、通信する場合、当然ネットワーク機密保護の問題が生じる。特に、ユーザのコンピュータが、例えばローカル基地局を有する無線リンク又はバンコックから米国への直接衛星リンクを介して通信する場合、無線機密保護、プライバシー及び認証が重要になる。無線メディアは無線データ通信を盗聴することを可能にする新しい機会を作り出す。適当な種類の無線受信機を持つている人はだれでも盗聴することが可能であり、実際この種の盗聴は探知できない。さらに、無線メディアは壁やドアの通常の物理

4

的制約によって阻むことができないので、無線メディアによる活発な侵入も達成することが比較的容易である。

【０００３】

【発明が解決しようとする課題】前述のように本発明は、ネットワークへの無許可アクセスを防止するための方法及び装置と、無線データ通信のプライバシー並びに通信当事者の認証の両方を備えている機密保護通信プロトコルを提供する。

【０００４】

【課題を解決するための手段】本発明は、移動無線データ処理装置とネットワークに結合された基地（固定ノード）データ処理装置間に機密保護通信リンクを与えるするための方法及び装置を提供する。この移動無線データ処理装置は、ランダムに選んだ呼び掛け値（ＣＨ1）及びサポートされている共用キーアルゴリズム（「ＳＫＣＳ」）のリストと共に基地データ処理装置にホスト認証（ＣＥＲＴ＿Ｍｏｂｉｌｅ）を送信する。基地データ処理装置は、委託された認証機関（ＣＡ）でディジタル署名された認証を検証する。ＣＥＲＴ＿Ｍｏｂｉｌｅが有効でないならば、基地データ処理装置は接続の試みを拒否する。次に、この基地データ処理装置は、ＣＥＲＴ＿ＢＡＳＥ、乱数（ＲＮ1）及び選択されたＳＫＣＳのための識別子を送信する。基地データ処理装置はＲＮ1 値を保管し、ＣＨ1 値及び選択されたＳＫＣＳを移動無線データ処理装置によって基地データ処理装置に送信されたメッセージに付加する。次に、基地データ処理装置はこのメッセージに署名し、移動無線データ処理装置にこのメッセージに送信する。次に、移動無線データ処理装置はＣＥＲＴ＿ＢＡＳＥを確認し、認証が有効ならば、移動無線データ処理装置は基地データ処理装置の公開キー（Ｐｕｂ＿ＢＡＳＥ）の下にメッセージの署名を検証する。この署名は基地データ処理装置のメッセージを取り込み、このメッセージに移動無線データ処理装置が第１のメッセージに与えたＣＨ1 及び共用キーアルゴリズム（ＳＫＣＳ）のリストを付加することによって検証される。基地データ処理装置の署名が有効でないならば、通信の試みは打ち切られる。基地データ処理装置の署名が有効である場合、移動無線データ処理装置の私用キーの下にＥ（Ｐｕｂ＿Ｍｏｂｉｌｅ，ＲＮ1）を解読することによってＲＮ1 の値を決定する。次に、移動無線データ処理装置はＲＮ２及びセッションキー（ＲＮ1とＲＮ2 のＥＸ－ＯＲ）を発生し、Ｐｕｂ＿ＢＡＳＥの下にＲＮ２を暗号化する。移動無線データ処理装置は暗号化されたＲＮ２及びＥ（Ｐｕｂ＿Ｍｏｂｉｌｅ，ＲＮ1）を移動無線データ処理装置の私用キーで署名されたメッセージで基地データ処理装置に送信する。次に、基地データ処理装置はＣＥＲＴ＿Ｍｏｂｉｌｅから得られたＰｕｂ＿Ｍｏｂｉｌｅを使用して移動無線データ処理装置の署名を検証する。この移動無線データ処理装置の署名が検証されるならば、基地データ処理装置はその私用キ

5

ーを使用してE（Ｐｕｂ＿Ｂａｓｅ，ＲＮ2）を解読する。次に、基地データ処理装置はセッションキー（ＲＮ１とＲＮ２のＥＸ－ＯＲ）を決定する。移動無線データ処理装置及び基地データ処理装置は、セッションキーを使用して解読された暗号化されたデータを使用してデータ転送フェーズに入る。さらに、本発明はセッション中セッションキーを変更するための方法を提供し、大型のネットワークの場合、認証（ＣＡ）の複数の確認を使用する可能性を与える。

【０００５】

【実施例】

表記法及び用語法

後述する詳細な説明は、ネットワークに結合されるデータ処理装置の動作の記号表示によって一般に表されている。これらのプロセスの説明及び表示は、他の当業者に仕事の内容を最も有効に伝えるためにデータ処理技術に精通している業者によって使用される手段である。

【０００６】アルゴリズムは、ここでは一般に所望の結果に導く自己矛盾のないステップ順序として表されている。これらのステップは物理量の物理操作を必要とする。通常、これらの物理量は、記憶され、転送され、結合され、比較され、表示され、かつ別な方法で操作されることのできる電気信号又は磁気信号の形をとる。これらの信号をビット、値、要素、シンボル、動作、メッセージ、用語、数等と呼ぶことで、主に共通用法のため時々便利であることがわかる。しかしながら、これらの類似用語の全ては適切な物理量に関連すべきであり、これらの物理量に適用される単なる便宜上のラベルであることを覚えておくべきである。

【０００７】本発明では、参照される動作はマシン操作である。本発明の動作を実行するのに有用なマシンは汎用ディジタルコンピュータ又は他の類似装置を含んでいる。全ての場合、コンピュータ操作の方法操作と計算方法そのものとの区別は心にとめておくべきである。本発明は、一連のネットワークに結合されたコンピュータを操作し、他の所望の物理信号を発生するために電気信号又は他の物理信号を処理するための方法ステップに関するものである。

【０００８】本発明はまたこれらの動作を実行するための装置に関するものである。この装置は特に必要とされる目的のために構成されるか又はこの装置は選択的に作動されるかあるいはコンピュータに記憶されるコンピュータプログラムによって再構成される汎用コンピュータを備えている。ここに記載されている方法／プロセスステップは本質的に特定のコンピュータ又は他の装置に関連されていない。さまざまの汎用機はここに示されている教義によるプログラムと共に使用され、必要とされる方法ステップを実行するために専用装置を構成することはより使利であることがわかる。種々のこれらのマシンに必要とされる構成は下記の説明から明らかである。

6

【０００９】下記の説明では、非常に多くの特定の項目が、本発明の完全な理解を与えるために、システム構成、代表的メッセージ、無線装置及び基地局等のように示されている。しかしながら、本発明はこれらの特定の項目なしで実施されることも当業者には明らかである。他の場合、周知の回路及び構成は本発明をわかりにくくしないために詳細に記載されていない。さらに、「知る」、「検証する」、「調べる」、「見つける」、「決定する」、「呼び掛ける」、「認証する」等のような正確な用語が本明細書で使用され、技術用語であると見なされる。コンピュータ又は電子システムの擬人化と見なされるこれらの用語の使用は、このシステムの機能を簡単にするため人間に類似する属性を有するように参照する。例えば、なにかを決定するような電子システムへのここでの参照は、電子システムがここでの教義によりプログラム化かされるかさもなければ修正されることを記述することの単に記述法である。前述の機能を日常の人間の属性と混同しないように注意すべきである。これらの機能はあらゆる意味でマシン機能である。

【００１０】典型的なハードウェア

図1は本発明によるデータ処理システムを示している。３つの主要な構成要素を備えているコンピュータ１が示されている。これらのうち第1の構成要素はコンピュータ１が他の部分間と適当に構成された形の情報を通信するために使用される入出力（Ｉ／Ｏ）回路2である。さらに、コンピュータ１はI／Ｏ回路2に結合された中央処理装置（ＣＰＵ）３及びメモリ４を含んでいる。これらの構成要素は、大抵の汎用コンピュータで典型的に見出される要素である。実際、コンピュータ１はデータ処理装置の広いカテゴリーを表すことを意図されている。また、周知のようにデータ及びコマンドをコンピュータ１に入力するキーボード５が図1に示されている。メッセージ発生・送受信回路7はまた、他のデータ処理装置とコンピュータ１とを通信可能にするためにI／Ｏ回路２を介してコンピュータ１に結合されている。例えば、図1では、コンピュータ１は図示のように無線送信機8を使用する他のデータ処理装置と通信する移動装置である。しかし、ここではコンピュータ１はネットワークに直接結合される。Ｉ／Ｏ回路2に結合されるラスタディスプレイモニタ６が示されている。このラスタディスプレイモニタ６はは本発明によりＣＰＵ3で発生された画像を表示するために使用される。周知の種類の陰極線管（ＣＲＴ）又は他の種類のディスプレイがディスプレイ６として使用される。

【００１１】本発明の目的

本発明のプロトコルの設計目的と無線移動装置及び基地局のプロトコルスタックの配置とが多数の要求によって決められる。主要な要求は、本発明のプロトコルスタックの機密保護機能の配置が、既存有線ネットワークへの統合であることである。非常の多数のネットワークアプ

7

リケーションは既存の有線ネットワークの世界で動作している。このアプリケーションは、典型的にネットワークでなんらかの機密保護レベルを持っている。この機密保護は、ある意味で、有線ネットワークの物理的機密保護によって与えられる。あいにく、無線メディアはいかなる物理的保護も有していないため、無線ネットワークを採り入れることは物理的ネットワークが提供する固有の保護を否定する。既存のソフトウェアアプリケーションのベースを少なくとも有線ネットワークを介して行ったと同様に安全に機能させるため、本発明は無線リンクそのものを機密保護する。

【００１２】２つの他の選択肢、アプリケーション層の端点間の機密保護及びトランスポート層の端点間の機密保護は、既存の有線ネットワークへの統合のための不適当に与えられた要求を考慮に入れられる。この統合の意義は、有線ネットワークの非常に多数の既存のノードが変えられないようにされるべきであるということである。移動ポータブル計算装置が有線ネットワークのノードと同一のレベルのネットワークアクセスを有する必要があるべきならば、アプリケーション層又はトランスポート層のいずれかに基づく端点間の機密保護を規定することは、全部の固定ノードネットワークのソフトウェアベースを修正する必要があるだろう。

【００１３】技術的背景のために、リンクの機密保護と端点間の機密保護との違いは図2に示されている。移動コンピュータ１０は基地装置１２と無線通信を行なう。この移動コンピュータ１０及び基地装置１２は図1に図示されるようなコンピュータシステムを備えている。基地装置１２はネットワーク１４の固定ノードである。ゲートウェイ１６は、図示のようにネットワーク１４、１８間で通信できるように設けられている。固定ノードデータ処理装置２０、２４は前記ネットワーク１８に結合されている。リンクレベル機密保護方は、移動コンピュータ１０と基地装置１２間の無線リンクが機密保護されていることを必要とする。ネットワーク１４、１８並びにゲートウェイ１６のための既存の機密保護機構は機密保護された無線リンクを付加することによって影響を及ぼされることを必要としない。端点間の機密保護機構では、移動コンピュータ１０は固定ノード（例えば、固定ノード２０）と直接通信する。それによって、移動コンピュータ１０は、ネットワーク１４、１８の各固定ノード及び移動ノードためのソフトウェアの全てが互換性があり、同一レベルのネットワーク機密保護を達成するように品質を高める必要がある。

【００１４】ネットワークの全てのノードが端点間の機密保護機構と互換性があるように改良されることが可能であるとみなされている動作環境では、実際、リンク機密保護は必要ない。これは、明かに非常に大きい集合的なネットワーク、即ちインターネットような大きな多重構成のネットワークでは可能でない。図2に示された構

8

想に採り入れられたリンクレベル機密保護方は既存の有線ネットワークのソフトウェアの品質を高めることを必要としないようにする。無線リンクそのものは機密保護されており、したがって全てのネットワーク、有線ネットワーク＋無線ネットワークの機密保護は有線ネットワークだけの機密保護と同様である。

【００１５】リンクレベル機密保護方は端点間機密保護機構を除外しないことが望ましい。このような機構は、リンクプロトコルに加えて付加的な機密保護プロトコルを処理することによってリンクレベル機密保護と共存することができる。図2に示される方法は、無線ネットワークが配備されるが、むしろ端点間機構によって全ネットワークを機密保護することが経済的意味をなす時点で端点間の機密保護を与える負担がかからない。

【００１６】リンク層は少なくとも２つのマシン、例えば移動コンピュータ１０、基地装置１２と固定ノード２０間の通信を含む。複数のユーザは単一のリンク層で典型的に多重化されるので、リンク層でのユーザの概念は厳密には適当でない。例えば、移動ユーザは無線リンクを介して幾つかのユーザと同時に通信する。これらの「会話」の全ては同一のリンク層の上部で多重化される。リンク層そのものは典型的な無線ネットワーク＋有線ネットワークにおける多くのホップのうちの一つのホップだけである。この状態が図3に示されている。図3に示するように、移動装置２５はネットワーク３０に結合される基地装置２７と無線通信する。この基地装置２７はネットワーク３０に結合される多くの固定ノードの一つ（例えば、固定ノード３２）である。ネットワーク３０とネットワーク３６間に結合されるゲートウェイ装置３４はそれぞれのネットワークに結合されるノード間での通信を可能にする。例えば、ネットワーク３６に結合される固定ノード３８は、ゲートウェイ装置３４を介して固定ノード３２と通信するか又は基地装置２７を通して移動装置２５と通信する。

【００１７】端点間機構は規定されていないので、ユーザの認証はそれによっては支配されない。これらの機構は無線リンクを介して主に通信するので、したがって、残されたものはノード間（又はマシン間）認証である。マシン間認証は、概念的にはリンク層の機密保護プロトコルにふさわしい。

【００１８】本発明のシステムの他の設計目的は、認証が相互認証を含んでいるということである。即ち、無線リンクの両端（移動装置２５及び基地装置２７）が互いに認証することが望ましい。唯一の許可された移動計算装置がネットワーク資源へアクセスする。同一の工業パークにある競争者の状態を考えるならば、基地装置２７を認証することも必要である。一人の競争者の基地局は他の競争者に属するようなふりをできないようにすべきである。相互認証はこの目的に役立ち、後述する本発明によって提供される。

9

【００１９】本発明の他の目的は、共用キー暗号学の将来の進歩を利用することができることに関して柔軟性を有することである。機密無線製品の全ての版間で相互運用を可能にする必要がある。

【００２０】本発明の概観

本発明は、プライバシー及び認証を達成するために公開キー暗号化技術（W.DiffieとM.Hellman著「暗号学の新しい方向」、IEEE Transactions on Information Theory、IT-22:644-645、1976を参照）及び共用キー暗号化技術の両方を使用する。公開キー暗号化はセッションキーセットアップ及び認証を行うために使用される。共用キー暗号化は本発明のプロトコルのプライバシーの態様を与えるために使用される。

【００２１】本発明のプロトコルの各関係するノードは公開キー／共用キー対を発生する。私用キーはキー対の所有者によってしっかりと保有される。公開キーは機密保護チャネルを介して委託された認証機関（ＣＡ）に付託される。ＣＡは関連情報を調べ、公開キーが、身元が知られており、信用できるだれかによって実際に提出されているかを確かめる。公開キーが付託されるならば、付託する人が、公開キーが認証されるマシンに代わって信任を得ることができると想定される。認証は、ＣＡの私用キーを使用してディジタル署名された書類の形で、公開キーとマシンの（マシン名のような）論理識別子間の結合を含んでいる。

【００２２】各マシンに対する認証並びに私用キーの機密保護バックアップを得られるならば、移動装置及び基地装置は機密保護プロトコルに携わることができる。二人の当事者は認証を交換し、相互の呼び掛け応答プロトコルに携わる。このプロトコルは共用キーアルゴリズムの交渉を可能にする。これは、将来のプロトコルをより良い共用キー暗号システムに高めることを可能にし、この暗号システムが輸出のために異なる暗号アルゴリズムを必要とするならば、これはまた製品のＵＳ版と非ＵＳ版間の相互運用性をも可能にする。

【００２３】プロトコルもまたかなり進んだ機密性を備えている。基地装置又は移動装置のいずれかの公開・私用キー対の私用構成要素がある将来時点で拘束されるとするならば、この拘束は、その私用キーが拘束されているマシンによって交換された無線リンクデータを必ずしも拘束するものではない。このプロトコルは基地装置と移動装置との間の通信を拘束するために基地装置及び移動装置の私用キーの両方を拘束する必要がある。これは複数のキーのうちのいずれかのキーへの拘束よりもありそうにない事象とみなされている。

【００２４】本発明によれば、環境及び時間フレームのために長くされるか又は短くされることができるキーの長さについては何の仮定もない。

【００２５】

定義

10

この明細書のために下記の用語、交渉及び略語は下記の意味を有する。Ｅ（Ｘ，Ｙ）はキーＸの下のＹの暗号と解されるべきである。ＭＤ（Ｘ）は内容Ｘに関するメッセージ要約関数と解されるべきである。

認証機関の公開キー＝Ｐｕｂ＿ＣＡ

認証機関の私用キー＝Ｐｒｉｖ＿ＣＡ

移動ホストの公開キー＝Ｐｕｂ＿Ｍｏｂｉｌｅ

移動ホストの私用キー＝Ｐｒｉｖ＿Ｍｏｂｉｌｅ

基地局の公開キー＝Ｐｕｂ＿Ｂａｓｅ

基地局の私用キー＝Ｐｒｉｖ＿Ｂａｓｅ

移動ホストの認証＝Ｃｅｒｔ＿Ｍｏｂｉｌｅ

基地局の認証＝Ｃｅｒｔ＿Ｂａｓｅ

Ｓｉｇ（Ｘ，Ｙ）はキーＸを有するＹの署名と解されるべきである。ここで、Ｓｉｇ（Ｘ，Ｙ）＝Ｅ（Ｘ，ＭＤ（Ｙ））

署名（Ｘ，Ｙ）は得られる署名メッセージ｛Ｙ，Ｓｉｇ（Ｘ，Ｙ）｝を表している。

【００２６】本発明の機密保護プロトコル

次に、図4と図5、６のフローチャートとを参照すると、接続開始時間に、有線ネットワークへの接続を要求する移動装置１００は、そのホスト認証（Ｃｅｒｔ＿Ｍｏｂｉｌｅ）、１２８ビットのランダムに選ばれた呼び掛け値（ＣＨ１）及びサポートされた共用キーアルゴリズム（「ＳＫＣＳ」）のリストを基地装置１０５に送信する。

【００２７】サポートされた共用キーアルゴリズムのリストは、基地装置１０５との共用キーアルゴリズム（例えば、ＦＥＡＬ－３２，ＤＥＳ，ＩＤＥＡ等）の交渉を認める。共用キーアルゴリズムは後続のデータパケットを暗号化するために使用される。共用キーアルゴリズムの交渉は、例えばプライバシーモジュールの国内版と外国版間の相互運用を可能にすることができる。認証は下記の情報を含んでいる。

｛連続番号、有効期間、マシン名、マシン公開キー、ＣＡ名｝

認証＝署名（Ｐｒｉｖ＿ＣＡ，認証内容）

【００２８】認証のフォーマット及び符号化は、ＣＣＩＴＴＸ．５０９（ＣＣＩＴＴ勧告Ｘ．５０９（１９８８），「ディレクトリー認証フレームワーク」参照）及びプライバシー強化メール（ＰＥＭ）（S.Kent,「Privacy Enhancement for InternetElectronic Mail: Part Certificate-Based Key Management",RFC 1422,BBN,February 1993; B.Kaliski,「Privacy Enhancement for Internet Electronic Mail:Part : Key Certification and Related Service",RFC 1424,BBN,February1993を参照）に規定されている認証のフォーマットと同一であるように選択されている。これにより、移動装置１００及び基地ステーション１０５はＸ．５００及びＰＥＭによって要求される同一の認証インフラストラクチャーからのてこの作用を行なうことを可能にする。

11

【００２９】メッセージ要約（ＭＤ）関数はホスト認証（Ｃｅｒｔ＿Ｍｏｂｉｌｅ）の内容で計算され、委託された認証機関（ＣＡ）によってディジタル署名される。署名はＣＡの私用キーの下でＭＤ（認証内容における非逆ハッシュ関数）を暗号化することによって達成される。これは、認証（Ｃｅｒｔ＿Ｍｏｂｉｌｅ）の内容を認証するが、この内容を私用にしない。認証に基づくキー管理及び認証発行の主題の詳細は、ＲＦＣ１４２２及び１４２４（S.Kent,「Privacy Enhancement forInternet Electronic Mail: Part Certificate-Based Key Management",RFC1422,BBN,February 1993; B.Kaliski,「Privacy Enhancement for Internet Electronic Mail:Part : Key Certification and Related Service", RFC 1424,BBN,February 1993 を参照）とＣＣＩＴＴ基準Ｘ．５０９を参照されたし。

【００３０】有線ネットワークに結合することを要求する移動装置１００から基地装置１０５への第1のメッセージは下記に示されるような情報を含んでいる。

メッセージ＃１．移動装置→基地装置

｛Ｃｅｒｔ＿Ｍｏｂｉｌｅ，ＣＨ１，ＳＫＣＳのリスト｝

ＣＨ１はランダムに発生された１２８ビット数である。共用キーアルゴリズムのリストはアルゴリズム識別子及びキーサイズの両方を含んでいる。

【００３１】メッセージを結合させるようにするこの要求を受信すると、基地装置１０５はＣｅｒｔ＿Ｍｏｂｉｌｅを有効にしようと試みる。これはＣｅｒｔ＿Ｍｏｂｉｌｅの内容のＭＤを独立して計算をすることによって行なわれ、署名されたＭＤのＣＡの公開キーの下でこれと暗号解読とを比較する。これらの二つの値が一致するならば、この点で基地装置１０５は、移動装置１００もまた認証Ｃｅｒｔ＿Ｍｏｂｉｌｅに与えられている公開キーに関連している私用キー（Ｐｒｉｖ＿Ｍｏｂｉｌｅ）を所有しているかどうかは知らないけれども、認証は有効である。

【００３２】認証が無効であるならば、基地装置１０５は接続の試みを拒否する。認証が検証されるならば、基地装置１０５はその認証について応答するだろう。乱数ＲＮ１は、移動装置１００の公開キー及び、基地装置１０５が移動装置１００によって与えられるリストの中から選んだ共用キー暗号システム（ＳＫＣＳ）の下で暗号化される。基地装置１０５は後で使用するために内部にＲＮ１を保管する。メッセージの署名を計算するために、基地装置１０５は呼び掛け値ＣＨ１及び共用キー暗号システムの両方をそれが送出するメッセージに付加する。

【００３３】ＳＫＣＳは、移動装置１００によってメッセージ＃１に提案された共用キーアルゴリズムの集合と基地装置１０５がサポートする集合との共通部分から選択される。基地装置１０５は、それが二つの集合の共通

12

部分から最も安全であると考えるＳＫＣＳアルゴリズムを選択する。キーサイズは常に、移動装置１００が提案し、基地装置１０５が選択されたアルゴリズムためにサポートすることができるキーサイズの最小値まで下がって交渉する。

【００３４】メッセージ＃２．基地装置→移動装置

｛Ｃｅｒｔ＿Ｂａｓｅ，Ｅ（Ｐｕｂ＿Ｍｏｂｉｌｅ，ＲＮ１），選択されたＳＫＣＳ

Ｓｉｇ（Ｐｒｉｖ＿Ｂａｓｅ，｛Ｅ（Ｐｕｂ＿Ｍｏｂｉｌｅ，ＲＮ１），選択されたＳＫＣＳ，ＣＨ１，ＳＫＣＳのリスト）｝

【００３５】図3を参照し続けると、選択されたＳＫＣＳは選択されたアルゴリズム及び関連するキーサイズの両方を識別する。メッセージに付加された署名は、それがメッセージの本体部分でなく、むしろプロトコルに内在するなにかを含んでいるので、メッセージの通常の署名と異なる。

【００３６】最初に、移動装置１００は、前述のＣＡの公開キー及びディジタル署名検証手順を使用して基地装置１０５の（ＣＥＲＴ＿Ｂａｓｅ）の認証を検証する。認証が有効であるならば、移動装置１００は、基地装置１０５の（Ｐｕｂ＿Ｂａｓｅ）の公開キーの下でメッセージの署名を検証する。

【００３７】署名は、基地装置のメッセージを取り込み、かつそれに、移動装置１００が第1のメッセージに送信したＣＨ１及び共用キーアルゴリズムのリストを付加することによって検証される。署名検証のためのリストの含意によってメッセージ＃１が未署名で送信されることを可能にする。攻撃者が、元のメッセージを妨害し、かつ攻撃者自身のリストを挿入することによって共用キーアルゴリズムのリストを弱めたいならば、これは第2のメッセージを受信する際、移動装置１００によって検出されるだろう。署名が一致するならば、基地装置１０５は認証されたと考える。さもなければ、基地装置１０５は詐称者と考えられるか又は元のメッセージがみだりに変更されているのではないかと思うい、かつ移動装置１００は接続の試みを打ち切るだろう。

【００３８】値ＲＮ１は移動装置１００の私用キーの下でＥ（Ｐｕｂ＿Ｍｏｂｉｌｅ，ＲＮ１）を暗号解読することにより移動装置で得られる。次に、移動装置１００は他の乱数ＲＮ２を発生し、セッションキーとして値（ＲＮ１とＲＮ２とのＥＸ－ＯＲ）を使用する。

【００３９】認証フェーズを完了し、かつキーＲＮ２の第2の半分と基地装置１０５とを通信するために、移動装置１００は、Ｐｕｂ＿Ｂａｓｅの下に値ＲＮ２を暗号化し、これをメッセージに送信する。このメッセージは、移動装置１００がメッセージ＃２で得られる元の暗号化されたＲＮ１値を含んでいる。署名が移動装置１００の私用キーを使用して移動装置１００で計算されるため、第3のメッセージにＥ（Ｐｕｂ＿Ｍｏｂｉｌｅ，Ｒ

13

Ｎ１）を含めることは移動装置１００を認証するのに役立つ。

【００４０】メッセージ＃３．移動装置→基地装置

｛Ｅ（Ｐｕｂ＿Ｂａｓｅ，ＲＮ２），Ｓｉｇ｛Ｐｒｉｖ＿Ｍｏｂｉｌｅ，｛Ｅ（Ｐｕｂ＿Ｂａｓｅ，ＲＮ２），Ｅ（Ｐｕｂ＿Ｍｏｂｉｌｅ，ＲＮ１）｝｝｝

【００４１】図4 及び図5 、６に示されるように、基地装置１０５はメッセージ＃１におけるＣｅｒｔ＿Ｍｏｂｉｌｅから得られるＰｕｂ＿Ｍｏｂｉｌｅを使用するメッセージの署名を検証する。この署名が検証されるならば、移動装置１００は認証されたホストと考えられるか、さもなければ移動装置１００は侵入者と考えられ、基地装置１０５は接続の試みを拒否する。

【００４２】データ転送フェーズに入る前に、基地装置１０５はそれ自身の私用キーを使用してＥ（Ｐｕｂ＿Ｂａｓｅ，ＲＮ２）を暗号解読する。基地装置１０５はまた、セッションキーとして（ＲＮ１とＲＮ２とのＥＸ－ＯＲ）を使用する。キーに対してＲＮ１を（単に使用することに対抗するように）２つのランダム値がキーに対して使用される理由は、これは、複数の移動装置の内の一つの私用キーが妥協させられるならば、起こり得る損害を制限するためである。この方法は、拘束されるべき基地装置１０５と移動装置１００間の以前のトラフィックに対して基地装置及び移動装置の私用キーの両者の拘束を必要とする。

【００４３】両方のキーの半分は等しい長さで完全にランダムであるので、ＲＮ１ 又はＲＮ２ のいずれかを知ることは、攻撃者にセッションキー（ＲＮ１とＲＮ２とのＥＸ－ＯＲ）について絶対何も知らせない。これは、使い捨ての暗号帳がワンタイムキーとしてもう一方を使用してＲＮ１ 及びＲＮ２ の各々に対して計算されるためである。

【００４４】接続の試みが成功すると、相互認証が起こり、セッションキーが得られる。

【００４５】図示のように、図4 でクロスハッチされているメッセージフィールドは、私用キー（ディジタル署名のために）又は公開キー（セッションキーの構成要素を保護するために）のいずれかを私用して暗号化される部分である。図のアンダーラインは、アンダーラインされたフィールドが署名ブロックの唯一の部分であり、メッセージそのものではないという事実を示している。メッセージ2 の署名は3 つの明確な目的にかなう。第1 の目的はメッセージ＃２を認証すること、第2 の目的はメッセージ＃１の呼び掛け応答として役立つこと、第3 の目的は（ＳＫＣＳのリストを含ませることによる）メッセージ＃１を認証することである。これは公開キー暗号システムの使用を最小にする。それによって、プロトコルが制限される計算資源でプラットホーム上を作動させることを最適化する。それにもかかわらず、本発明のプロトコルはなお強い機密保護保障を備えている。

14

【００４６】公開キー暗号システムの計算法上で費用がかかる部分は、典型的には私用キー動作である。ＲＳＡ（ＲＳＡ Ｄａｔａ Ｓｅｃｕｒｉｔｙ，Ｉｎｃ．ＰＫＣＳ＃１－＃１０，１９９１を参照）のような公開キー暗号システムは、署名検証プロセス及び公開キー暗号プロセスを最少にするために典型的には複数のキーを選択する。したがって、プロトコルの効率を評定するために、私用キー動作の全数が計数される。移動装置１００は2 つの私用キー動作を実行する。第1 の動作はＲＮ１を暗号解読する動作、第2 の動作はメッセージ＃３に署名する動作である。基地装置１０５もまた2 つの私用キー動作を実行する。第1 の動作はメッセージ＃２に署名する動作、第2 の動作はメッセージ＃３から暗号解読する動作である。したがって、全部計算上費用がかかる（私用キー）動作は本発明では4 つの動作だけである。

【００４７】本発明の教義を使用して、メッセージキーで交換されるキーは、実際2 つの異なるキーである。このキーはデータ転送の各方向に対するものである。暗号が付加ストリームモードで動作される場合、これはキーストリームの再使用を防止する。本明細書で後述されるプロトコル符号化は、各方向に対する２つのキーがいかに識別されるかを識別する。

【００４８】データパケット

データパケットに対する主要な問題は、パケット遺失がある場合のデータパケットの暗号解読性を保持することである。データパケットは、無線リンクでノイズ又は反射のため遺失されるか又は乱れて到達するかもしれない。本発明によれば、解決方は共用キー暗号及びその作動モードに依る。付加ストリーム暗号の場合、擬似ランダムストリームと同期したままでいるために、各サイドの６４ビットの「メッセージ識別」フィールドは各パケットの開始に明文で送信される。この「メッセージ識別」フィールドは以前送信された全バイト数を含んでいる。これにより、検出されないか又は改悪されたかあるいは乱れている無線リンクパケットが存在する場合、付加ストリーム暗号で正しい動作を可能にする。

【００４９】暗号フィードバックモード又はカウンタ駆動モードのＤＥＳの場合、「メッセージ識別」は最後のパケットの暗号テキストの最後の６４ビットである。出力フィードバックモードのＤＥＳの場合、「メッセージ識別」は単に送信された６４ビットブロック数の計数である。「メッセージ識別」の長さは及びその意味は、共用キーアルゴリズム及びその動作モードの選択に必然的に含まれる。

【００５０】データパケットの完全性チェックは、暗号化されるパケットデータの一部である３２ビットチェックサムフィールドで各パケットを追跡することによって行なわれる。これは、データパケットに対して完全性及びプライバシーの両方を備えているが、再生保護を備えていない。データパケットに対する再生保護は重要であ

15

ると考えられない。幾つかの再生の試みがＴＣＰ／ＴＰ４等のような比較的高い層プロトコルによって拒否されることはありそうである。再生は通常の（良好な）データグラム環境で可能であるので、攻撃者はデータパケットの再生を加えることによって悪意ある結果を得ることを期待できない。

【００５１】本発明のキー変更プロトコル

変更キーメッセージ交換は、基地装置１０５又は移動装置１００のいずれかによって開始されることができる。基地装置１０５は下記のようにキー変更を開始する。

１．基地装置１０５→移動装置１００

署名（Ｐｒｉｖ__Ｂａｓｅ，｛Ｅ（Ｐｕｂ__Ｍｏｂｉｌｅ，Ｎｅｗ　ＲＮ１，Ｅ（Ｐｕｂ__Ｍｏｂｉｌｅ，ＲＮ１）｝）

２．移動装置１００→基地装置１０５

署名（Ｐｒｉｖ__Ｍｏｂｉｌｅ，｛Ｅ（Ｐｕｂ__Ｂａｓｅ，Ｎｅｗ　ＲＮ２，Ｅ（Ｐｕｂ__Ｂａｓｅ，ＲＮ２）｝）

移動装置１００がキー変更を開始するならば、手順は下記のようになる。

１．移動装置１００→基地装置１０５

署名（Ｐｒｉｖ__Ｍｏｂｉｌｅ，｛Ｅ（Ｐｕｂ__Ｂａｓｅ，Ｎｅｗ　ＲＮ２，Ｅ（Ｐｕｂ__Ｂａｓｅ，ＲＮ２）｝）

２．基地装置１０５→移動装置１００

署名（Ｐｒｉｖ__Ｂａｓｅ，｛Ｅ（Ｐｕｂ__Ｍｏｂｉｌｅ，Ｎｅｗ　ＲＮ１，Ｅ（Ｐｕｂ__Ｍｏｂｉｌｅ，ＲＮ１）｝）

【００５２】値（（Ｎｅｗ__ＲＮ２）と（Ｎｅｗ__ＲＮ１）とのＥＸ－ＯＲ）は新しいキーとして使用される。どちらもより最新である値ＲＮ１及びＲＮ２は、常に最後のキー交換から得られる。このキー交換は最初の接続設定又は最後のキー交換メッセージからである。

【００５３】たとえどの装置（基地装置又は移動装置）がキー変更を開始しても、ＲＮ１は常に基地装置１０５によって発生されたキーの一部を参照し、ＲＮ２は常に移動装置１００によって発生されたキーの一部を参照する。変更キーメッセージはＳＫＣＳを再開始するのに役立つ。

【００５４】各サイドは、メッセージの署名を検証し、ＲＮ１及びＲＮ２とその内部に記憶された値と比較する。署名が検証されないか又はＲＮ１／ＲＮ２値が内部に記憶された値と一致しないならば、キー変更メッセージが変更されるだろう。メッセージがキー変更の履歴に敏感であるため、これによりキー変更メッセージが再生されることを防止する。キー変更メッセージが検出なしで再生されることができるならば、この結果2つの本物の端点で一致しないキーが得られ、したがって攻撃のサービスタイプの簡単な否認を可能にする。このような攻撃は、前述のようなタイプのキー変更メッセージによって排除される。

16

【００５５】本発明により、連続番号を再分類することなしにキー変更メッセージが再生されることを防止する。連続番号は停電及びマシン再始動の全域で記憶される必要があるので、連続番号はプロトコル実行で動作するのには長たらしい。

【００５６】複数のＣＡによる動作

本発明は単一のネットワークの範囲にわたるＣＡによって前述された。大型のネットワークの場合、単一のＣＡは全てのネットワークノードに役立つことができる。このような場合、ＣＡの階層が使用される。このようなＣＡの階層がＣＣＩＴＴＸ．５０９及びＰＥＭ　ＲＦＣに詳細に記載されている。ＣＡの階層が使用される場合、プロトコルは下記のように修正される。メッセージ＃２は基地局の認証だけを含んでいない。そのかわりとして、メッセージ＃２は、移動装置が基地局の認証を検証することを可能にする認証パスを送信する。この認証パスは、移動装置の認証が発行されたＣＡから開始されるように基地局によって構成される。基地局は有線ネットワークに接続されているので、基地局にこのようなパスを構成することを可能にするネットワークデータベース（ディレクトリサービス）へアクセスする。移動装置１００は全ての可能な認証パスを知るように構成されることができないので、自分自身の認証を送信することが単に必要とされる。これにより、移動装置１００の構成は簡単にすることができる一方、ＣＡの階層の形で複数のＣＡを許すという柔軟性をなお可能にしている。

【００５７】複数のＣＡを含めることにより必要とされる他の修正は、移動装置１００が、認証パスにおける各ＣＡに対して認証取り消しリスト（ＣＲＬ）の最新情報を取り入れたコピーを有することを期待されることができないということである。ＣＲＬは、認証された公開キーに対応する私用キーが妥協される可能性に適応させる必要がある。このような起こり得る事態では、その認証は、不正に入手したものとしてリストされるか又は取り消されるかする必要がある。ＣＲＬは、ＣＡによって取り消された全ての認証をリストにしている不正入手リストである。基地局はまた認証パスにおける各ＣＡに対してＣＲＬを供給する責任を有する。ＣＲＬはＲＦＣ１４２２に詳細に記載されている。したがって、新しいメッセージ＃２は下記のようになる。

【００５８】メッセージ＃２．基地装置１０５→移動装置１００

｛Ｃｅｒｔ__Ｐａｔｈ，ＣＲＬのリスト，Ｅ（Ｐｕｂ__Ｍｏｂｉｌｅ，ＲＮ１），選択されたＳＫＣＳ，Ｓｉｇ（Ｐｒｉｖ__Ｂａｓｅ，｛Ｅ（Ｐｕｂ__Ｍｏｂｉｌｅ，ＲＮ１），選択されたＳＫＣＳ，ＣＨ１，ＳＫＣＳのリスト｝）｝

【００５９】プロトコル符号化

プロトコルの符号化を詳細に説明するために、ＡＳＮ．

17

1(「CCITT勧告X.208(1988),「Specification of Abstract Syntax Notation(ASN.1)" を参照) におけるメッセージを明細に述べる。この符号化は、X.509セクション8.7に明記されているようにASN.1 BER(「CCITT勧告X.209(1988),「Specification of Basic Encoding Rules for ASN.1"を参照) のDERの部分集合を使用して実行される。

【0060】メッセージ#1.

```
Message-1::=SEQUENCE{
mobileCert          Certicate
challengeToBase     OCTET STRING,
listOfSKCS          SEQUENCE OF AlgorithmIdentifier}
```

【0061】メッセージ#2.

```
Message-2::=SEQUENCE{
baseCertpath        CertificationPath,
listOfCRLs          SEQUENCE OF
CertificateRevocationList,
baseToMobileRN1     OCTET STRING,
mobileToBaseRN1     OCTET STRING,
chosenSKCS          AlgorithmIdentifier,
sigalg              AlgorithmIdentifier,
message2sig         BIT STRING}
```

【0062】メッセージ#3.

```
Message-3::=SEQUENCE{
baseToMobileRN2     OCTET STRING,
mobileToBaseRN2     OCTET STRING,
sigalg              AlgorithmIdentifier,
message3sig         BIT STRING}
```

【0063】アルゴリズム識別子、認証及び認証パスはX.509に明記されている。認証取り消しリストはRFC 1422に規定されている。メッセージ#2及びメッセージ#3はmessage2sig及びmessage3sigをそれぞれ計算するために使用される署名アルゴリズムを識別する。これは、ハッシュアルゴリズム及び公開キー暗号システムの両方を含んでいる。これは、署名がメッセージそのものに完全に含まれているフィールドに対して計算されないことを除いては、SIGNED ASN.1 MACRO OF X.509と精神において互換がある。

【0068】理想化されたプロトコル

18

*【0064】集約すると公開キー暗号標準(PKCS) (RSA Data Security,Inc.PKCS#1-#10,June 1991参照) として公知であるRSADSI 社からの標準セットは幾つかのディジタル署名及び公開キー暗号システムの両方を明記している。これらの例はRSA暗号及びRSA公開キー暗号システムと共にMDSを含んでいる。これらは認証及びプロトコル関連ディジタル署名及び公開キー暗号のために使用されている。

【0065】本発明のプロトコルのプルーフ

プロトコルの機密保護はバロウーズ、アバディ及びニードハム(M.Burrows,M.Abdi,R.Needham,「A Logic Authentication",DES SRC Research Report #3,Feb22,1990を参照) によって開発された認証論理を使用して証明される。記載されているような形式主義は本発明のようなサーバーのないプロトコルを記述するにおいて制限を有する。この制限は公開キー認証の検証で行なわれなければならない。認証から論理的に得られることができる全ては、CAは「KaはAを代表している」と一度言うということである。CAが、認証が有効であることをなお信じるかどうかについて何も言えることは何もない。実際、これは認証取り消しリスト及び認証そのものの有効期間によって処理される。元の形式主義を信じるように一度言うことを進めようとする唯一の方法がステートメントの新しい特性の使用によるものであるため、これは限界である。サーバーのないプロトコルでは、サーバーが必ずしも通信時間に使用可能でないため、このような新しい保障を備えることができない。

【0066】この問題に注目すると、それと反対にステートメントがなければ、認証は新しいものであると仮定される。プロトコルを解析するために、プロトコルの理想化された版が最初に得られる。これを行なうために、形式主義に存在してない要素を除く。これは全ての明文テキスト通信並びに共用キーアルゴリズムの交渉を含んでいる。最初に、分解された具体的なプロトコルが提供され、続いて理想化された版が提供される。(アバディ等により使用されているのと同一の表記法) Aは移動装置100で、Bは基地装置105である。CH1はNaである。

【0067】具体的なプロトコル

【数1】

$$\text{メッセージ1:A} \longrightarrow \text{B} \qquad \{\xrightarrow{K_a} A\}_{K_{ca}^{-1}}, N_a$$

$$\text{メッセージ2:B} \longrightarrow \text{A} \qquad \{\{\xrightarrow{K_b} B\}_{K_{ca}^{-1}}, \{RN1\}_{K_a}, N_a\}_{K_b^{-1}}$$

$$\text{メッセージ3:A} \longrightarrow \text{B} \qquad \{\{RN2\}_{K_b}, \{RN1\}_{K_a}\}_{K_a^{-1}}$$

【数2】

メッセージ1:A ──> B　$\{\overset{K_a}{\longmapsto} A\}_{K_{ca}^{-1}}$

メッセージ2:B ──> A　$\{\{\overset{K_b}{\longmapsto} B\}_{K_{ca}^{-1}}, (A \overset{RN1}{\longleftrightarrow} B), N_a\}_{K_b^{-1}}$

メッセージ3:B ──> A　$\{(A \overset{RN2}{\longleftrightarrow} B), \{RN1\}_{K_b}\}_{K_b^{-1}}$

【0069】プルーフ仮説

【数3】

a) $A \models \overset{K_a}{\longmapsto} A$

b) $A \models \overset{K_{ca}}{\longmapsto} CA_K$

c) $A \models (CA \Rightarrow \longmapsto B)$

d) $A \models \#(N_a)$

e) $A \models A \overset{RN2}{\longleftrightarrow} B$

f) $B \models \overset{K_b}{\longmapsto} B$

g) $B \models \overset{K_{ca}}{\longmapsto} CA_K$

h) $B \models (CA \Rightarrow \longmapsto A)$

i) $B \models \#(RN1)$

j) $B \models A \overset{RN1}{\longleftrightarrow} B$

k) $CA \models \overset{K_a}{\longmapsto} A$

l) $CA \models \overset{K_{ca}}{\longmapsto} CA$

m) $CA \models \overset{K_b}{\longmapsto} B$

n) $A \models (B \Rightarrow A \overset{RN1}{\longleftrightarrow} B)$

o) $B \models (A \Rightarrow A \overset{RN2}{\longleftrightarrow} B)$

【0070】プルーフ

メッセージ＃2、仮説b）及び仮説c）、メッセージの意味規則及び法律適用権規則並びにCert Bは新しいと仮定されているという主張から、下記の式を得る。

【数4】

$$A \lhd \{\{\overset{K_b}{\longmapsto} B\}_{K_{ca}^{-1}}, (A \overset{RN1}{\longleftrightarrow} B), N_a\}_{K_b^{-1}}$$

$$A \models \overset{K_b}{\longmapsto} B$$

【0071】メッセージの意味の規則を適用すると、下記の式を得る。

【数5】

$$A \models B \mid\!\sim \{\{\overset{K_b}{\longmapsto}\}_{K_{ca}^{-1}}, (A \overset{RN1}{\leftrightarrow} B), N_a\}$$

【0072】仮説d）及び一回だけの検証規則から下記の式を得る。

【数6】

$$A \models B \models (A \overset{RN1}{\leftrightarrow} B)$$

【0073】法律適用権規則及び仮説n）を適用すると、

【数7】

$$A \models (A \overset{RN1}{\leftrightarrow} B) \quad \text{—結果1}$$

【0074】メッセージ＃1、仮説g）及び仮説h）、メッセージの意味規則及び法律適用権規則並びにCert Aは新しいと仮定されているという主張から、下記の式を得る。

【数8】

$$B \models \overset{K_a}{\longmapsto} A$$

【0075】メッセージ＃3から、下記の式を得る。

【数9】

$$B \lhd \{(A \overset{RN2}{\leftrightarrow} B), \{RN1\}_{K_a}\}_{K_a^{-1}}$$

【0076】メッセージの意味の規則を適用すると、下記の式を得る。

【数10】

$$B \models A \mid\!\sim ((A \overset{RN2}{\leftrightarrow} B), \{RN1\}_{K_a})$$

【0077】一回だけの検証規則及び仮説i）を適用すると、

【数11】

$$B \models A \models (A \overset{RN2}{\leftrightarrow} B)$$

【0078】法律適用権規則及び仮説o）を適用すると、

【数12】

$$B \models (A \overset{RN2}{\leftrightarrow} B)$$

【0079】結果1及び上記結論から、下記の2つの結果を得る。

【数13】

$$A \models (A \overset{RN2}{\leftrightarrow} B)$$

$$B \models (A \overset{RN1}{\leftrightarrow} B)$$

【0080】Kab=RN1とRN2とのEX－ORであるので

【0081】仮説e）及び仮説j）並びに2つの結果から下記の式を得る。

【数14】

21

$$A \models A \overset{K_{ab}}{\leftrightarrow} B$$

$$B \models A \overset{K_{ab}}{\leftrightarrow} B$$

【００８２】これらは認証プロトコルの目的である。認証形式主義の論理は、今後の機密保護のような問題を取り扱っていないが、しかし、これは本発明のプロトコルの付加的目的である。また、本発明では、同期化クロックの使用は避けられる。同期化クロックを必要とすることはそれに関連した多くの問題を有する（ W.Diffie,P.C.V.Oorschot,M.J.Wiener,“ Authentication and Authenticated Key Exchanges",in “ Designs,Codes and Cryptography,pages 107-125,Kluwer Aademic Publishers,1992を参照）。呼び掛け応答機構を使用することはこれらの問題を避ける。仮説i ）は、セッションキー（ＲＮ１）の一部が認証目的、すなわち認証プロトコルの他の望ましい属性のために使用されているという事実を明白にする。

【００８３】仮説n ）及び仮説o ）は、各辺が受け入れ可能なキー構成要素を発生するために他方の辺の権限の信用を表していることにおいて異常である。当事者の一人又は二人がセッションキーを発生する責任があるため、これはサーバーのないプロトコルに必要である。これは、偶発性及び予測不可能性の適切な特性を有するキーを選ぶために両辺の権限のプロトコルにおいて説明されていない要求の反映である。

【００８４】したがって、無線ネットワークためのプライバシー及び認証のためのシステム及び方法が開示されている。本発明は図1 ～図6 で識別される幾つかの特定

22

の実施例に関連して記載されていると同時に、前述の記載に照らして多くの他の実施例、修正例及び変更例が可能であることは当業者に明らかである。

【図面の簡単な説明】

【図1】　本発明の教義を組み入れているデータ処理システムを示している図、

【図2】　移動無線ノードの使用を組み入れている多重ネットワークシステムにおけるリンク機密保護と端点間機密保護間の差異を示している図、

【図3】　多重ネットワークに結合された幾つかのユーザと通信する移動ユーザを示している図、

【図4】　本発明による機密保護リンクを確立するために移動装置及び基地装置によって実行されるステップ順序を概念的に示している図、

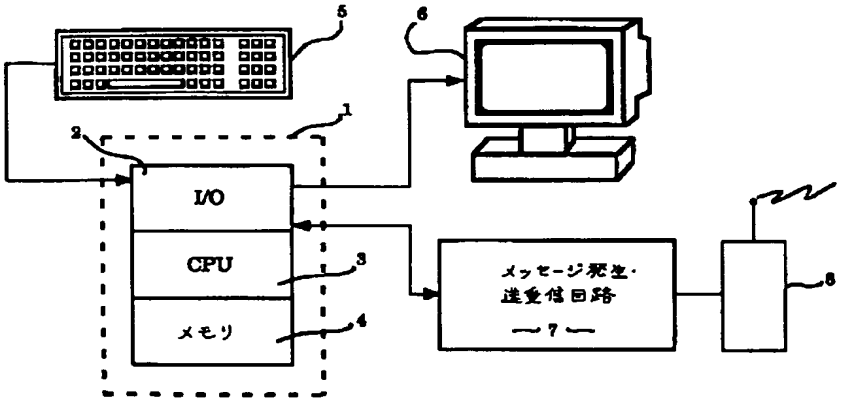
【図5】　図4 に概念的に示されている移動装置及び基地装置によって実行されるステップのフローチャートを示している図、

【図6】　図4 に概念的に示されている移動装置及び基地装置によって実行されるステップのフローチャートを示している図である。

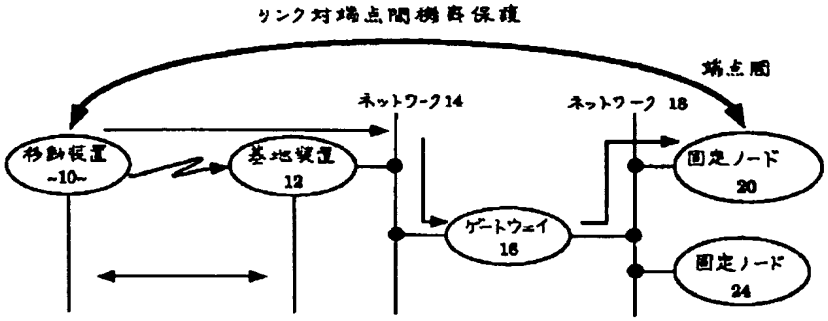
【符号の説明】

１…コンピュータ、２…入出力回路、３…中央処理装置、４…メモリ、５…キーボード、６…ラスタディスプレイモニタ、７…メッセージ発生・送受信回路、８…無線送信機、１０、２５、１００…移動装置、１２、２７、１０５…基地装置、１４、１８、３０、３６…ネットワーク、１６、３４…ゲートウェイ、２０、２４、３２、３８、４０…固定ノード。

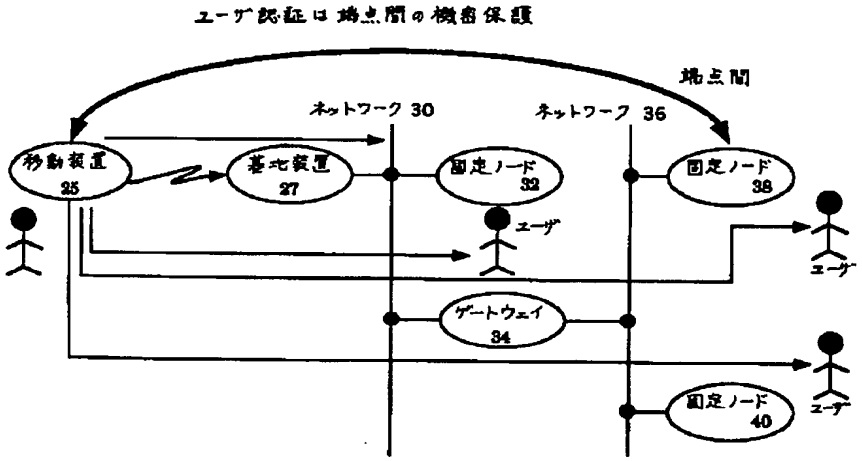
【図1】



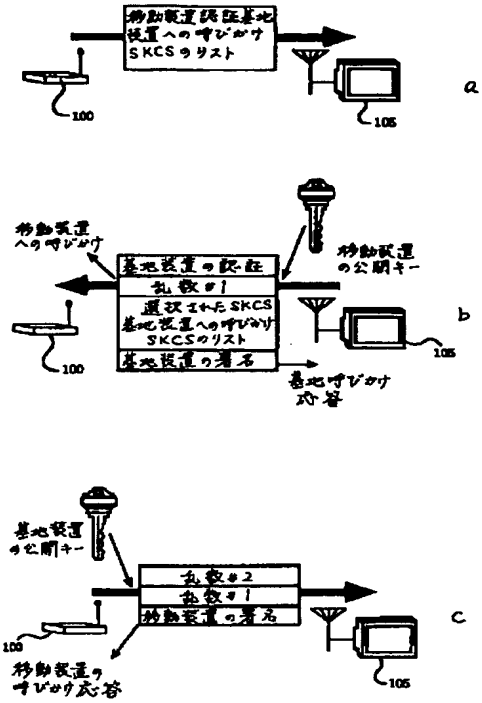
【図2】


リンク対端点間機密保護
端点間
ネットワーク14
ネットワーク 18
移動装置
-10-
基地装置
12
ゲートウェイ
16
固定ノード
20
固定ノード
24

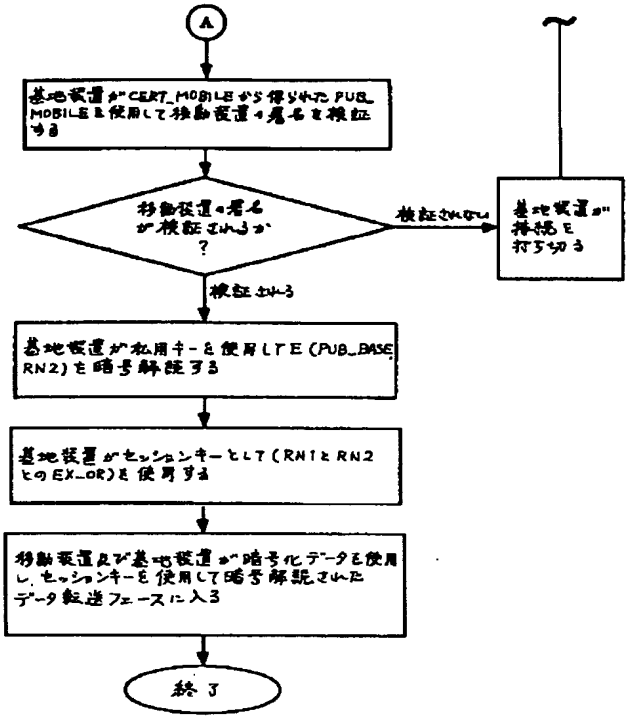
【図3】


ユーザ認証は端点間の機密保護
端点間
ネットワーク 30
ネットワーク 36
移動装置
25
基地装置
27
固定ノード
32
固定ノード
38
ユーザ
ユーザ
ゲートウェイ
34
ユーザ
固定ノード
40

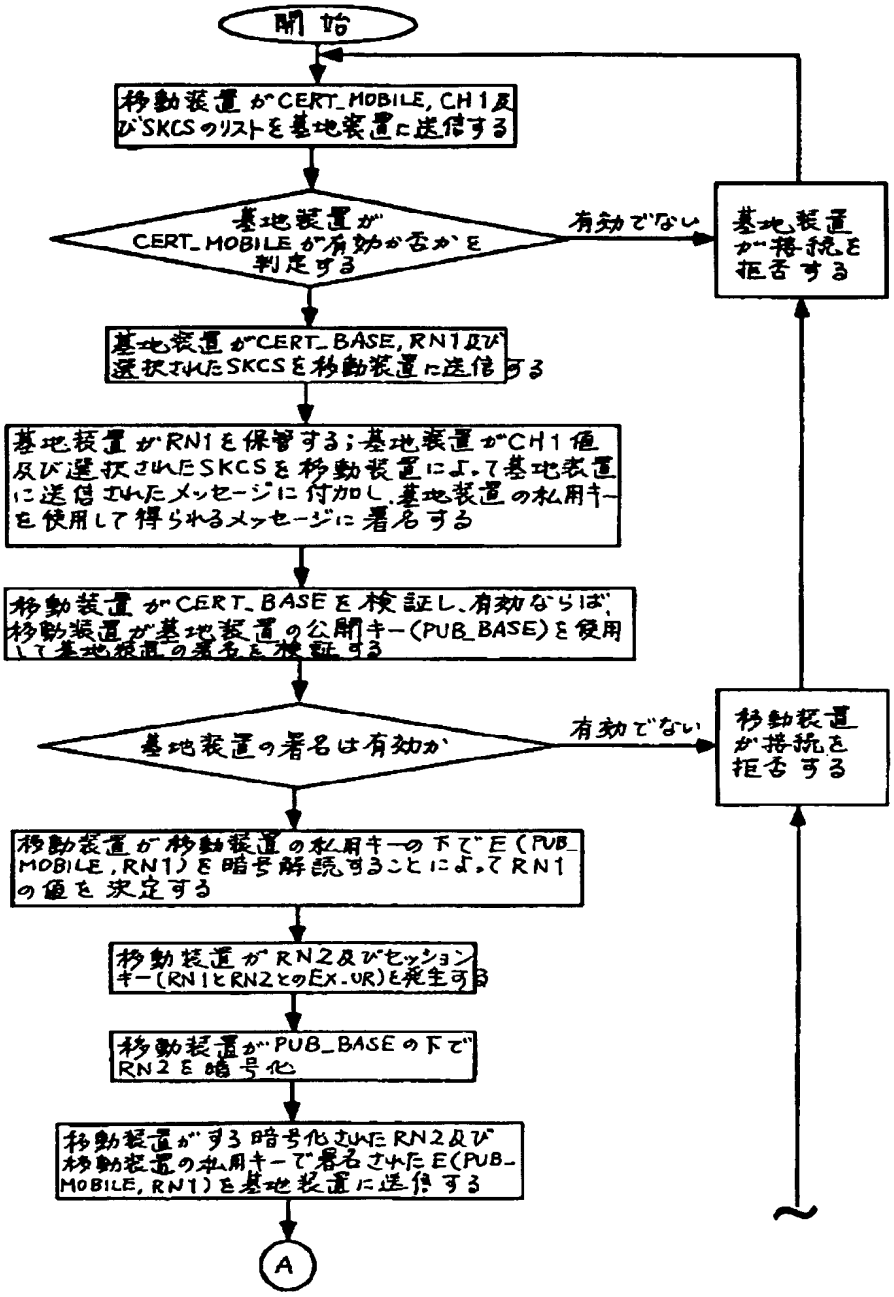
【 図4 】


移動装置認証基地装置への呼びかけ
SKCSのリスト
100
105
a
移動装置への呼びかけ
基地装置の記憶
乱数#1
選択されたSKCS
基地装置への呼びかけ
SKCSのリスト
基地装置の署名
移動装置の公開キー
基地呼びかけ応答
b
基地装置の公開キー
乱数#2
乱数#1
移動装置の署名
移動装置の呼びかけ応答
c

【 図6 】


A
基地装置がCERT_MOBILEから得られたPUB_MOBILEを使用して移動装置の署名を検証する
移動装置の署名が検証されるか？
検証されない
基地装置が接続を打ち切る
検証される
基地装置が私用キーを使用してE(PUB_BASE RN2)を暗号解読する
基地装置がセッションキーとしてT(RN1とRN2とのEX_OR)を使用する
移動装置及び基地装置が暗号化データを使用し、セッションキーを使用して暗号解読されたデータ転送フェーズに入る
終了

【図5】



フロントページの続き

(51)Int.Cl.[6]	識別記号	庁内整理番号	FI	技術表示箇所
H04K 1/00		Z		

(72)発明者　アシャー・アジズ
アメリカ合衆国　94555　カリフォルニア
州・フレモント・タナガー　コモン・ 4180